Speed must be viewed and treated like the fundamental element it is. But by its very nature, security slows things down. When you’re in the security business, you’re fundamentally in the business of slowing people down, and that’s a horrible business to be in. Security must harness the power of speed to secure information while protecting against cyberattacks at the same rates.

Simply put, all cybersecurity must be extremely fast.

Security without speed is a losing proposition. In fact, slow security is often no security. Good security strategy must be based on leveraging speed, specifically

- Raw speed to detect and mitigate attacks in real time
- Processing capacity with more sensors, more data, and more insights to parse data more efficiently and find the smallest anomalies in system functionality

“Speed is at the nucleus of the cyberfrontier.”

Roland Cloutier, ADP

“Greater connectivity, faster transmission and processing speeds, and machine algorithms result in faster and potentially more accurate decisions.”

Scott Charney, Microsoft
• Forward compatibility to create the headroom to implement future solutions that could involve even greater speed

Good security strategy must achieve these goals with as little impact as possible on the speed users have come to expect and demand. That’s because in addition to the operational reason for speed, there is a practical reason: Users aren’t willing to wait.

A consistent consequence results from that user impatience paired with cybersecurity techniques that don’t feature speed as a fundamental component: Slow security solutions get shut off, either because they are too cumbersome or because they simply can’t keep up. A security solution that lacks speed and thus is turned off provides zero benefit. Thus, slow cybersecurity techniques become greater impediments than benefits.

If organizations are forced to adopt tools that do not meet the needs and standards of fast data transfer, the odds are that not only will those organizations become less safe, but they will carry that lack of safety to every point of connectivity they share, endangering other organizations.

Acknowledging the inherent conflict between security and speed requires us to strategically design how, where, and when to slow things down, while maintaining and preserving as much velocity and efficiency as possible.

When it comes to cybersecurity, without speed, there is nothing. Users will, however, embrace a solution with speed as its key component.
Context is king when providing tangible models of reference to complex issues like cybersecurity. Even as security practitioners, we are faced with an onslaught of information, intelligence, data points, and other exceptional information with a need for action or decision, but we often lack the availability of context to make sense of the environmental settings that help us make great decisions.

WHAT DO WE MEAN BY SPEED?

As we begin to discuss speed as a binding strategy and guiding principle for approaching cybersecurity, we must take the time to truly understand the implications and context of the meaning of speed as a multifaceted component of the threat, of what we are protecting, of how we protect, and of the impact on our ability to be successful.

Speed is in fact at the nucleus of the cyberfrontier. As a term, it can be considered a noun (the rate at which something is measured for movement) or a verb (describing an action of movement). In either case, when linked to the defense of technology, it is speed that dictates our plans, actions, and, often, outcomes. It is speed that supports measures of priority along with residual risk measures. And it is speed that impacts basic program considerations such as cost, services, and urgency.

We’ll now explore key areas of speed as a binding strategy and the key strategic elements that you can focus on to help you make better decisions, deliver better results, and have a greater impact in protecting your charge.

HOW SPEED IMPACTS SECURITY

Living in a digitally connected ecosystem of business, societies, and global economies that operate at the speed of light means that the factors and issues that determine how and what we protect are
like a living, breathing organism. It is always thinking, consuming, and growing in many different ways. First, the environment you work in is not a controlled and managed architecture of systems and software encased in a protected data center with limited exposure. From the interconnection of data platforms between organizations to the extended components of the Internet, and even through the introduction of self-learning and decision-making software, digital infrastructures and operations are affected by the speed at which the globe is connected. To further complicate these scenarios, the human element cannot be forgotten. Decisions and actions made by humans can readily and starkly change the environment you protect through a limitless number of potential social and physical interactions.

Speed is also a critical element in the pace of change. Technology from a pure business asset perspective is often measured in years. Today, however, through the adaptation of advanced technology for criminal means, some cyberdefensive technologies may have a realistic effectiveness of only less than a year, and in some cases, days. The speed of the threat actor, your own technology environment, and your ability to defend it is entirely predicated on the speed of change. That pace of change also includes the necessary changes to our speed of making decisions. The critical actions of stopping, impeding, disrupting, and responding to cybersecurity risk and events that affect privacy in a digital world force us to make rapid and accurate decisions never required in previous decades. New methods of data acquisition and analysis for decision support are critical aspects of creating these new strategies for success in a digital age.

Finally, speed is a significant financial lever. Beyond the normal cost considerations of time to acquisition, time to deployment, and other accounting mechanisms that manage the total operating cost of programs, projects, and operations, the reality is that the speed of the next generational digital economy and the infrastructures you protect will essentially shorten the lifespan of any given technology or capital investment in your cybersecurity defense architecture. Technology in a normalized information technology portfolio is rationalized into a three- to five-year investment with a depreciation scheme that has been the standard for multiple decades. However, with the advancement of the criminal use of technology, protective and defense technology lifespans have been greatly reduced.
Through artificial intelligence (AI) and machine learning (ML), and the use of intelligence services, criminals can now identify, recalculate, and react to technology in record time, sometimes reducing the expected lifetime of a cybersecurity asset and investment from years to months or even days.

This chapter focuses on strategies to understand, plan for, and affect the impact of speed on how you think about and execute your responsibilities in defending your business or agency.

THE STRATEGIC IMPERATIVES

You may think that to align to the change in speed, you simply have to move and act faster. Although in some cases that is true, there are better ways to approach operational acceleration and excellence in the face of dynamic change than fighting speed with more speed. How we think, act, and instrument our protection portfolio and operations are all key aspects in making this dynamic shift to operational enablement in the age of speed. The reality is that the world, technology, and threats will only continue to gain momentum, and if the only tool in your toolbox is an ability to run faster, you'll soon realize the limits of that way of thinking. Strategic imperatives such as risk, intelligence, transparency, and action-based decision making are additional tools that when learned, practiced, and mastered will create new capabilities that are far more effective and sustainable than speed itself.

THE PURPOSE OF YOUR MISSION

Before you can decide how to best apply your newfound strategic tools, you must know the “why” of the “how and when” you will need to use them. Every business, industry, and organization is different. The reasons you need to protect your organization and how you protect it are important. Why you do what you do feeds into your organizational risk appetite, defines your value at risk, and informs key decision-making points such as the level of accuracy needed versus speed and financial investments. Working through a normalized risk process, or even something as simple as sitting down with your business leaders and discussing the downstream residual impact of cybersecurity failure, will help inform and shape your mission parameters. Are you part of critical infrastructure? Would
intellectual property loss ruin your business? Can your business ecosystem outside your control cause irreparable damage? These questions and many others should be the foundational elements of how you describe your “business of security” and what your mission focus is. In turn, as you begin to consider the implication of the speed used against you and the speed that will help you accelerate your effectiveness, a deep understanding of your mission imperatives in alignment with the following five critical areas of planning will ensure your success in the hyperconnected and hyperspeed world in which you operate:

1. Understand your environment. Your success depends on your direct ability to succeed within the environment in which you operate. To do that, you need to understand your environment through transparency, knowledge, and access. This includes crucial elements such as understanding your critical assets, a holistic understanding of the resources and technology deployed through a comprehensive configuration management database (CMDB), and data flow diagrams that detail how information flows through your business. Just as important is the understanding of your third-party ecosystem, your supply chain, and how your services are in effect an integrated component of your customers’ supply chains. Your ability to quickly understand the impact of any given event through this level of transparency is a fundamental component to being able to think and act quickly.

2. Drive safely at high speed. Your business success depends on speed to market and speed to respond. Your job is to get everyone there safely. This sense of speed enablement, or acting like the brakes on the car so your business is confident to go faster, requires a mature risk process. Effective risk programs have tiers of risk considerations and actions that create broad bands of flexibility and enable decision making based on preselected and informed risk formulas that serve as guiding principles. Spending time developing those mechanisms and allowing them to mature, educating your business, and just as importantly, educating your team will empower and enable all levels of the organization to recognize and facilitate business-based risk decision making at speed.
3. Plan ahead. Your opposition is well funded, utilizing capabilities and decisioning guiderails that are faster than yours. As in an old-fashioned gunfight, the first one to put lead on the target wins. This means that you need to be comfortable with rapid decision making based on accumulated knowledge rather than absolutes and have a “gun belt” of premade decisions, actions, and plans on your side. For instance, if you have a ransomware incident that is less than x% contained, do you shut down your data center? If you are suffering a financial crimes attack, will you call law enforcement, and if so, what agency and what is their number? Simple efforts such as tabletop exercises or defining preplanned partners significantly add to your ability to react fast in times of crisis. Prepositioned decision making agreed to by your leadership also ensures that your business will understand, support, and expect clear action and leadership from you when needed.

4. See the big picture. You need over-the-horizon threat modeling. I think everyone would agree that seeing a speeding train coming at you is better than getting run over by one. Unfortunately, too many people concentrate too myopically on their own operating environment and never look up long enough to see the train coming down the tracks. The use of intelligence services, information-sharing partnerships, and other mechanisms that give you a view outside your business into adjacent industries, like competitors or aligned ecosystems, are great ways to measure and prepare for the potential impact of issues not yet affecting your business. This greatly enhances your time to prepare, plan, and react to situations and opportunities that too often are missed because of insular behaviors.

5. Make the most of limited resources. Managing a business with limited return on investment (ROI), no profit, and smaller teams takes a different approach. Not every industry has the mission criticality of a nuclear power plant or the financial resources of the financial sector, and most of us never will. But just because we can’t build large operating teams doesn’t mean there aren’t methodologies we can put forth to make us more nimble and adaptable. For instance, sometimes less is more. Often, many of the services we use are not employed on a constant basis, and
thus the costs associated with maintaining them or the skills needed to maintain them are wasted. Why not consider third-party contracting support for those services? And that’s not just for limited services. If there are opportunities to leverage or utilize an ecosystem of providers to deliver core services at a lower cost, or to use automation and cloud-based services to maintain a more current and manageable portion of your operations, why not consider them? Sometimes, using simplified capabilities rather than an entire offering allows you to have those capabilities most necessary to react fast for the most critical issue, while maintaining a profit and loss (P&L) reasonable for your business.

THE SCIENCE OF RACING: ACCELERATION, DECELERATION, HARD BRAKING, AND KNOWING WHEN TO APPLY EACH

The natural attraction of humans to speed has been a part of our history from the time we could walk upright. Whether by foot across land, in boats on the water, or being pulled by an animal, speed was a part of our ancestors’ survival plan, social fabric, and continuing intellectual quest. In modern times, billions of dollars are spent on the sport of racing just about everything. But one of the most complex integrations of speed and humans is that between human and automobile. Whether it is for the sport of a high-speed thrill around a track, across the land in amazing road races, or as a part of our survival on the part of those who protect society by driving fast to protect and save lives, people have gotten good at driving automobiles fast.

As with anything else, there is a science, skill, and methodology to manipulating a vehicle into speeds faster than the norm, and the failure of not understanding that typically has a devastating effect. For example, not understanding at what point of a curve to accelerate or brake can cause you to roll your vehicle, not understanding the dynamic force of an object in motion will cause you to lose control, and not understanding acceleration inertia delay will cause you to lose your race.

In cybersecurity, the same is true of a leader managing the objective of being effective in the face of speed. There are tools, skills, and a science to creating an effective approach to enable
organizations to move fast and defend against an ever-changing opponent. Many elements can assist you in delivering against that objective, but the following are practical skills that you can start using today.

ELEMENTS OF FORCE MULTIPLICATION

The military has been using the term *force multiplication* since the beginning of organized military doctrine hundreds of years ago. The concept is relatively straightforward: Apply additional assets to your common core operating capability (people), and it accelerates and expands their effectiveness. For example, give an army the asset of intelligence, and its operating impact will be greater than it was before it had that information. Give ground forces the capability of GPS location, and they will be faster and more accurate than they were with the same amount of core resources prior to that technology.

As a practitioner in digital infrastructure leadership, you can enable your organization to strategically focus on the need for speed through the same use of force multiplication. By aligning to the elements of speed that most affect your mission scope, you can add levers that will multiply the abilities of your resources. Perhaps it’s intelligence, automation, or new technology. In some cases, it may be the use of a third party or the ability to have access to data. Whatever it is, you have an opportunity to manipulate and accelerate your current capabilities to meet the need for speed through the simple application of resource elements, resource combinations, and resource alignment.

Inertia

Books have been written on the laws of motion, and great strides in science have been gained through the study of motion and speed. The fundamental laws of motion still apply, and the truth of the principle that “things in motion stay in motion” is undeniable. In the context of speed, cybersecurity, leadership, and your job, the ability to act fast starts with the basic ability to act. In this arena, inertia is counter to growing in capability and speed over time. Often, we wait too long to enable our organizations with capabilities because of limited funding, resources, or just wanting a plan that is 100 percent...
complete every time. This approach is not helpful, nor is it necessary, because it will inevitably result in being too late to begin to create a necessary capability at the time it is most needed.

A simple tool in the development of operational effectiveness in the face of speed is to create supporting services, resources, and capabilities aligned with the scope of your mission that will be most applicable in the core areas of prevention, detection, response, and recovery. The idea is not to create these capabilities at 100 percent, but rather to have a baseline operating framework, knowledge, and understanding that can be refined and used over time. By maintaining this aggregate line-level capability, ensuring you and your organization understand it, adding it to your concept of operations, and knowing not only how it is applied but how to grow it, you can implement resources faster than if you were starting from scratch. Even though they may be minimal in normal operations, your ability to grow them fast and apply them faster will be significantly greater than if you had to start from the beginning.

Prioritization

A key capability often missing in an organization’s ability to execute at speed is its ability to prioritize. Although in our world, many if not most things seem to be equally critical, the reality is that there is always a pecking order and prioritization of action and attention, and recognizing that is crucial to making smart, informed, and rational decisions that enable speed. As an operational leader, you should always have these three priority lists on hand, updated, and ready to use in your decision-making process:

Critical Asset Protection Priorities. These are the assets, systems, processes, or functions that run your business. If you had only $100.00 to spend, what would you spend it on? This discussion should be inclusive of your business to ensure you understand what it takes to go to market, what enables your business to operate, and what key assets hold the most value to your company.

Risk Prioritization. This list is all about your focus. What projects are most critical to resolve your value-at-risk? Where can you deprioritize to affect other priorities, and where can you move resources to scale faster?
Urgent Action Defense Protocols. These are pre-negotiated/decided actions for when things go wrong. In layman’s terms, which part of the body can I cut off to save the head? When catastrophic issues occur, timely decisions are necessary to prevent further catastrophe. Who can order the shutdown of a business line, and when? What thresholds require automatic action, such as turning a data center dark? Who has the authority to call law enforcement if needed? The most critical part is to get these hard-to-make decisions on paper, including what would trigger them, and ensure agreement across the entirety of the business on how to execute them.

GETTING ON THE HIGHWAY AND GETTING UP TO SPEED

In an era in which digital enablement means digital impact at breakneck speeds, it is hard to forget that the bad guys only need to get it right once, and we are responsible for getting it right every time. The education, innovation, planning, convincing, implementation, and management of “all of these things” that enable us to protect our businesses or agencies (especially at scale) don’t lend themselves to the term *speed*. But that is exactly how we must retool our thinking and operations to ensure the digital success of a very digital economy. Through the five-step methodology of Learn, Test, Accelerate, Validate, and Repeat, we can continue to inch ourselves toward a more progressive capability that includes speed as a binding strategy to success.

Learn

Understand your organization’s ability to adapt to and operate within strategies that incorporate speed as a fundamental requirement, and work those job functions and requirements into every job description. Create opportunities for education, practice, and innovation for speed in delivery, change, response, and, just as importantly, decision making.
Test

Test your processes to ensure that they meet the speed requirements your mission prioritizes and your operating environment requires. Until they are put to the test, theories are just theories. Unless you test, stretch, and ensure your ability to adapt and respond at speed, you will be operating on false expectations, which never has a good outcome.

Accelerate

Incrementally add capabilities to drive acceleration. Perhaps it’s the use of automation in data collecting, or the use of automated analytics to churn through that data. Maybe it’s shedding old technologies, programs, or services that are not part of your priority list that enables you to act faster. Whatever it is, first understand why you are making the change and then create a measure to ensure that the change is meaningful and effective. Finally, hold yourself and your organization accountable to maintain that new capability.

Validate

Validation is the art of putting it all together. Once your organization is educated, instrumented, and ready to operate at high velocity, it’s time to validate it. There is nothing that stops a potential disaster from occurring in real time better than conducting tabletop exercises (TTXs) of issues, incidents, decision making, or just about anything that happens in your business or agency. In fact, not only are these great learning and adjustment opportunities, but they are also incredible team-building exercises. Knowing that I can trust my skills and the skills of those with whom I work instills a tremendous amount of confidence, which in turn helps us all run, act, and execute faster.

Repeat

Nothing in this new digital business ecosystem is stagnant. “Complacency kills” is one of the first things that military and law enforcement officers are trained on. If your situation is changing but your tools, technologies, practices, and capabilities are not, you will be at the losing end of any battle. Avoid complacency by implementing a life-cycle approach to reviewing and improving on your adaptation toward becoming a speed-based organization.
OPERATING LIMITS FOR YOURSELF AND OTHERS

None of this happens in a vacuum. Your ability to apply these principles, operate in a speed-enabled environment, and deliver services in a next-generation digital ecosystem depends on people. Part of your growth, and that of your business, will be to understand the strengths and weaknesses of people and their ability to execute and adapt over time. Speed has no place if it is not integrated as a binding component of your strategy, because an organization that attempts it without a thoughtful, purposeful, and well-planned approach will fail.

Finally, base your success in cybersecurity operations on an advantageous application of speed in how you think, understand, plan, and execute to the digital world around you.

ABOUT THE CONTRIBUTOR

Roland Cloutier – SVP and CISO, ADP

As staff vice president and chief security officer (CSO) of ADP, Roland Cloutier brings understanding and knowledge of global protection and security leadership to one of the world’s largest providers of human capital management solutions. With over 25 years of experience in the military, law enforcement, and commercial sectors, Cloutier is a leading expert in corporate and enterprise security, cyberdefense program development, and business operations protection. At ADP, Cloutier has functional and operational responsibility for cybersecurity, information protection, risk, workforce protection, crisis management, and investigative security operations worldwide.

Prior to ADP, Cloutier served as vice president and CSO of EMC, where he spearheaded protection of its worldwide business operations, including leadership of all information, business risk, crisis management, and investigative security operations across commercial and government sectors. He served as vice president of cybersecurity at AimNet Solutions. He has more than 14 years of experience in the military and federal law enforcement in global aerospace protection, fraud and diversion investigations, and special event protection, including an assignment at the 1996 Olympic Summer Games in Atlanta.
An old adage warns, “He who hesitates is lost.” Put another way, speed is essential. Indeed, speed is most often viewed in a positive light, connoting everything from exhilaration (fast cars), to competitive advantage (faster stock trades), to greater efficiency (airplanes over buses). Yes, there may be drawbacks (“haste makes waste”), but forward we rush.

In information technology, speed is often synonymous with increased productivity. Moore’s law, which noted that the number of transistors in a dense integrated circuit doubles approximately every two years, permits us to process more data in less time. Faster transmission speeds, from fiber to 5G, give us access to larger datasets in less time. Machine learning and AI permit us to leverage these other technologies and promise decisions that will be both better and faster.

While this paints a rosy picture, there is another adage about speed, one that conjures up notions of risk. Although it may be true that “he who hesitates is lost,” we are often cautioned to “look before we leap.” That is, we need to slow down and be more cautious when making decisions.

So, should we in fact look before we leap, even if those who hesitate are lost? Which piece of conventional wisdom is correct? Clearly, quickly embracing new technology can yield terrific benefits, even if new risks must be managed at the same time. But can speed be cause for alarm?

Which adage is correct depends on context, and in this regard, it may be helpful to consider three different, albeit simplified, scenarios. The first involves credit applications in which older processes are made more efficient through modernization; the second involves unlocking new, transformative capabilities through the introduction of autonomous vehicles; and the third involves international affairs and the potential use of autonomous lethal weapons.
In the area of financial transactions and the issuing of credit cards, we once asked humans to collect and analyze datasets and then make a binary decision about whether to grant credit. Two of these tasks—collecting and analyzing data—might be relatively time consuming and labor intensive, even if making the actual credit decision was relatively quick. In a post-computerized world, the process may be far more thorough (involving more data), happen far more quickly, and may all be done by machine. Simply put, greater connectivity, faster transmission and processing speeds, and machine algorithms have streamlined the process, resulting in faster and potentially more accurate decisions at lower cost. Yes, there are challenges with this approach, ranging from privacy concerns to biased datasets to faulty algorithms, but with appropriate controls and oversight, the risk is manageable.

More than just increasing transaction processing, the speed with which data can be collected, analyzed, and acted on may serve to protect both consumers and banks. For example, by more quickly analyzing spending patterns, banks can more quickly detect anomalous transactions and alert consumers of potential fraud. Perhaps more interestingly, banks themselves benefit from new computer security protections, particularly as they embrace cloud-based services. The reason is simple: In the cloud, we can harness new security capabilities that reduce security response times so that they more closely track the speed of malware distribution. This is best explained by example. Defenders of networks have long highlighted the importance of information sharing. Using the Financial Services Information Sharing and Analysis Center (FS-ISAC) as an example, if Bank A sees an attack, it notifies the ISAC. The ISAC notifies other banks, which then look for indicators of compromise on their networks. Other sectors have ISACs as well.

Although this model works well, it has challenges. First, it requires information sharing, which happens well in some sectors but not as well in others. Second, information distribution and analysis can take time. Third, the information may not flow to all players (for example, in the case of the financial sector, smaller banks may be less engaged). By contrast, as banks move to the cloud, the speed of response can increase dramatically. For example, Microsoft’s Advanced Threat Protection strips attachments from emails, runs
them in detonation chambers, and looks for malware. If found, that malware can be searched for throughout the cloud. This means if Bank A is attacked, all other banks—and other customers outside the financial sector—can quickly be protected from that attack. Simply put, protections can be broadly deployed to more entities without information-sharing delays. Moreover, as more customers move to the cloud, the amount of telemetry increases and protections improve. Thus, in the context of these financial transactions, speed provides significant benefits.

CONTEXT: AUTONOMOUS VEHICLES

Autonomous vehicles, which have started cruising the streets of major cities, offer a long list of benefits, including safer streets, more efficient use of vehicles leading to less congestion, increased mobility for seniors, and more. Data collection and analysis speeds are again critical, especially as vehicles analyze data on roads crowded with other cars, bikes, pedestrians, and traffic lights. It is also important that such technologies leverage the cloud (where data from multiple sources can be stored and analyzed) but also make “local” decisions without the latency caused by transmitting data to and from the cloud (this is called the “intelligent cloud/intelligent edge” model).

At the same time, we will be presented with new risks as the technology matures and perhaps comes under attack. Indeed, as of December 17, 2018, the California Department of Motor Vehicles had received 124 Autonomous Vehicle Collision Reports, and there have been reports of researchers hacking automated vehicles. Still, while autonomous vehicles may not be completely “safe,” they will, if correctly designed, undoubtedly be “safer”: Autonomous vehicles can process data far more quickly than humans, they will not panic in an emergency situation, and they are unlikely to be distracted by cell phones.

CONTEXT: AUTONOMOUS LETHAL WEAPONS

It is in the third scenario, international relations and autonomous lethal weapons, that speed may pose risks to humanity itself. That is a dramatic statement to be sure, but one that is not alarmist when the future of technology is considered in a military context.
The problem is that human thinking and the processes humans have established to manage their international affairs do not map to Moore’s law—we do not become exponentially faster over time.

In the last century, intercontinental ballistic missiles shortened military response times from days to minutes. Since then, the introduction of cyberwarfare capabilities has arguably reduced response times further. As General Joseph Dunford, the outgoing Chairman of the Joint Chiefs of Staff, noted in 2017, “The speed of war has changed, and the nature of these changes makes the global security environment even more unpredictable, dangerous, and unforgiving. Decision space has collapsed and so our processes must adapt to keep pace with the speed of war [emphasis added].” To take advantage of the remaining decision space, Dunford noted, there must be “a common understanding of the threat, providing a clear understanding of the capabilities and limitations of the joint force, and then establishing a framework that enables senior leaders to make decisions in a timely manner.” This suggests the need for greater pre-decisional planning, from collecting better intelligence about adversaries’ capabilities and intentions to better scenario planning so that decisions can be made more quickly.

At the same time that we attempt to adapt, we must also grapple with a fundamental question: As the need for speed increases, will humans delegate decision making—even in lethal situations—to machines? That humans will remain in the loop is not a foregone conclusion. With the creation of autonomous lethal weapons, some countries have announced new policies requiring a “human-in-the-loop” (see Department of Defense Directive Number 3000.09, November 12, 2012). Additionally, concerned individuals and organizations are leading calls for international treaties limiting such weapons (see https://autonomousweapons.org/). But as we have seen with cybersecurity norms, gaining widespread international agreement can be difficult, particularly when technology is new and countries do not want to quickly, and perhaps prematurely, limit their future activities. And as we have seen recently with chemical weapons, ensuring compliance even with agreed-upon rules can be challenging.
THE DIGITAL BIG BANG

THE RISK

The risk here is twofold. The first relates to speed: If decision times collapse and outcomes favor those who are willing to delegate to machines, those who accept delay by maintaining adherence to principles of human control may find themselves disadvantaged. Second, there is the reality that humans will, over time, come to trust machines with life-altering decisions. Self-driving cars represent one example of this phenomenon. At first, self-driving vehicles required a human at the wheel “for emergencies.” Later, automated vehicles with no steering wheel and no human driver were approved. While this may be, in part, because humans have proven to be poor at paying attention and reacting quickly in a crisis, experience and familiarity with machines may have also engendered complacency with automated vehicles, much as we have accepted technology in other areas of our lives. If this is correct, then humans may ultimately conclude that with decisional time shrinking, machines will make better decisions than the humans they serve, even when human lives are at stake.

ABOUT THE CONTRIBUTOR

Scott Charney – Vice President of Security Policy, Microsoft

Scott Charney is vice president for security policy at Microsoft. He serves as vice chair of the National Security Telecommunications Advisory Committee, as a commissioner on the Global Commission for the Stability of Cyberspace, and as chair of the board of the Global Cyber Alliance. Prior to his current position, Charney led Microsoft’s Trustworthy Computing Group, where he was responsible for enforcing mandatory security engineering policies and implementing security strategy. Before that, he served as chief of the Computer Crime and Intellectual Property Section (CCIPS) at the U.S. Department of Justice (DOJ), where he was responsible for implementing DOJ’s computer crime and intellectual property initiatives. Under his direction, CCIPS investigated and prosecuted national and international hacker cases, economic espionage cases, and violations of the federal criminal copyright and trademark laws. He served three years as chair of the G8 Subgroup on High-Tech Crime, was vice chair of the Organization of Economic Cooperation and Development (OECD) Group of Experts on Security and Privacy, led the U.S. Delegation to the OECD on Cryptography Policy, and was co-chair of the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency.